Internet et vie privée

Poullet, Yves

Published in:
Journal des Tribunaux

Publication date:
2001

Document Version
le PDF de l'éditeur

INTERNET ET VIE PRIVÉE : ENTRE RISQUES ET ESPOIRS [1]

Les caractéristiques même du réseau des réseaux que constitue Internet expliquent l'accroissement des risques encourus par nos libertés. Dans quelle mesure nos législations de protection des données permettent-elles une réelle protection contre ces risques nouveaux? De nouveaux droits ne sont-ils pas à consacrer et leur protection ne doit-elle pas faire appel à d'autres modes de protection, qu'il s'agisse d'autorégulation ou de la technologie elle-même?

I INTRODUCTION

1. — La toile d'Internet s'étend chaque jour : on parle aujourd'hui de plus de 400 millions d'internautes (2) et la croissance est exponentielle; les services offerts suivent la même courbe et le commerce électronique promet à chacun des services de plus en plus variés et ingénieux, mettant le monde à portée d'un simple clic. Dans le même temps, certains Cassandre décrient cet univers virtuel comme la fin de nos libertés et y voient un *panopticon* (3) global d'autant plus dangereux qu'insidieux et omnipotent. Cette ambivalence est ressentie chaque jour plus crucialement par les citoyens. Au pays d'Internet, les sondages (4) traduisent cette crainte de plus en plus réelle et réclament la prise de mesures réglementaires effectives (5). Notre propos est d'éclairer le débat actuel et de suggérer quelques pistes à l'heure où les autorités européennes ouvrent le chantier de la révision des deux directives instaurant un régime de protection de la vie privée (6) et à l'heure où quelques dossiers, tels notamment Echelon (7), la surveillance dans les entreprises de l'utilisation d'Internet par les employés (8) et les pratiques de *cybermarketing* (9), défraient la chronique.

2. — Quelles particularités du réseau expliquent le caractère neuf des débats ouverts par Internet en matière de vie privée? Quatre particularités (10) méritent d'être soulignées. La première est certes le caractère interactif du réseau. Il est loin le temps des bases de données nominatives souvent bien localisées et rassemblant une vaste collection d'informations. L'interactivité des réseaux et leur utilisation de plus en plus banalisée expliquent que nous soyons les premiers auteurs des traces qu'en permanence nous créons, tantôt par le dialogue avec un site web, tantôt par le déplacement de notre voiture équipée d'un G.P.S. (11), tantôt par l'utilisation de nos mobilophones désormais reliés à Internet (12). Ces traces que nous laissons consciemment ou inconsciemment peuvent être captées par de nombreux acteurs et enrichir, voire susciter la création de nombreux traitements. Sans doute, l'interactivité signifie-t-elle également le fait que nous puissions à tout moment effectuer des choix, renoncer à poursuivre une visite, nous identifier ou non, réclamer telle ou telle protection, consentir à tel ou tel traitement. Le consentement, corollaire possible de l'interactivité est sans doute un facteur majeur de la protection de nos libertés sur Internet. Nous reviendrons sur ce point (*infra*, n^{os} 14 et 15).

3. — La deuxième caractéristique d'Internet est l'ouverture du réseau et le nombre de services qu'il offre. Ouverture, dans la mesure où chacun peut s'y connecter, ce qui n'est pas sans poser le problème de confidentia-

(1) Le présent article reprend et développe les idées exprimées par l'auteur lors de la XXII^{e} conférence internationale des commissaires à la protection des données : « Towards an electronic citizenship », conférence tenue à Venise, les 28, 29 et 30 septembre 2000. Les idées y contenues représentent le point de vue personnel de leur auteur et n'engagent en aucune manière les institutions dont l'auteur est membre. La rédaction de cet article a bénéficié des travaux menés par l'auteur dans le cadre du Pôle d'attraction interuniversitaire (P.A.I.) « Société de l'information » financé par les S.S.T.C. du premier ministre.

(2) ... selon les chiffres de la Nua Internet Society (disponibles au site : *www.nua.ie/surveys/*).

(3) J. Boyle, Foucault *in Cyberspace, Surveillance, Sovereignty and Hard-wired Censors*, disponible à *www.wel.american.edu/pub/faculty/boyle/foucl.htm*.

(4) Cf. les sondages cités par le rapport « Courrier électronique et protection des données » présenté par Mme C. Alvergnat à la C.N.I.L. et adopté par cette institution le 14 octobre 1999 (rapport disponible sur le site de la C.N.I.L. : *www.cnil.fr*). Ces sondages indiquent que plus d'un Américain sur deux estiment que l'absence de protection des données sur le Net et en particulier l'envoi de courriers non sollicités représentent une nuisance sérieuse.

(5) C'est en tout cas l'avis de la Federal Trade Commission qui, le 15 mai 2000, concluait à la nécessité de prendre des mesures y compris législatives pour protéger la vie privée sur Internet (cf Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security, mai 1999, disponible sur le site de la F.T.C. : *www.ftc.gov/privacy/index.htm* où le lecteur trouvera d'autres rapports officiels de la F.T.C. en la matière).

(6) Les directives 95/46 dite générale et 97/66 dite télécom et vie privée sont en instance de révision. Pour la première, la révision a fait l'objet de simples déclarations d'intention. Pour la seconde, un texte a déjà été élaboré par la Commission et a fait l'objet d'un dépôt devant le Parlement. Cette proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (COM[2000]385 final) s'insère dans une série de propositions visant à l'adoption d'un cadre réglementaire pour les communications électroniques (n^{o} prop. : 10962/00 ECO 243 CODEC 617).

(7) A propos du réseau Echelon, le lecteur peut se référer au rapport d'expertise rédigé à l'attention du comité permanent de contrôle des services de renseignements, rapport produit par l'auteur lui-même et J.-M. Dinant, « Le réseau Echelon : Existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger? », publié dans le rapport annuel du comité au Parlement, 2000.

(8) Cette question a fait l'objet récemment d'une recommandation de la Commission belge de protection de la vie privée (C.P.V.P.) publiée sur le site de la Commission (*www.privacy.fgov.be*) : avis n^{o} 10/2000 du 3 avril 2000 relatif à la surveillance par l'employeur de l'utilisation de l'informatique sur les lieux du travail.

(9) Sur ces pratiques, lire l'article de T. Leonard, « E-commerce et protection des données à caractère personnel : quelques considérations sur la licéité des pratiques nouvelles de marketing sur Internet », rapport présenté au colloque de la V.U.B. du 31 mars 2000 (à paraître) (disponible sur le site *www.droit-technologie.org*). Cf. également, l'article de M. Walraeve, « The Cybermarketingmix and Privacy Issues », disponible sur le site Eclip (*www.eclip.org*) et l'ouvrage de ce dernier, *Privacy gescand*, Univ. Pers Leuven, 1999, 482 pages et L. Bergkamp et J. Dhont, « Data Protection in Europe and the Internet : an Analysis of the European Community's Privacy Legislation in the context of the World Wide Web », *E.D.I. Law Review,* 2001, à paraître.

(10) Sur ces caractéristiques d'Internet, lire de manière plus approfondie, Y. Poullet, « Internet et vie privée, nouveaux enjeux, nouvelles solutions », *in Proceedings of the Stresa Conference, in Societa dell'informazione tutela della reservatezza*, 16/17 mai 1997, Giuffre Ed., Milano, 1998, pp. 49-72.

(11) Global Positioning System...

(12) Par la technologie du W.A.P.

lité des messages qui circulent sur ce réseau encore peu sûr (13). Ouverture également du fait que les messages qui y sont publiés, ainsi mon *curriculum vitae*, telle ou telle activité ou publication que j'y mentionne, ma photo, peuvent être retrouvés en particulier grâce à la puissance des moteurs de recherche et utilisés à d'autres fins que celles pour lesquelles ils ont été présentés sur le Net. Enfin, l'ouverture du réseau se traduit par la possibilité de « sauter » d'un site à l'autre et ceci sans fin, ce qui, nous l'avons dit, entraîne la multiplication des traces en des lieux différents.

4. — La dimension globale des réseaux et la multiplication des flux transfrontières suscitent quelques inquiétudes : la première naît de la constatation de la disparité des systèmes de protection des données, voire de l'absence de protection dans certains pays par lesquels transitent les données ou dans lesquels sont installés les sites de destination des messages. La seconde est illustrée par le cas Echelon, réseau d'écoute des messages transitant par satellite mis en place par certains services étatiques de renseignements (14). Le fait que des messages, y compris purement nationaux, puissent être captés à l'occasion de leur transit par satellite par des puissances étrangères démontre les limites de notre souveraineté (15) et la relative impuissance des régimes de protection mis en place par les Etats, en particulier européens, à l'heure où les réseaux ne connaissent plus de frontières.

5. — A ces caractéristiques d'Internet, s'ajoute celle de l'opacité : la littérature récente (16) a démontré la multiplication des traitements dits invisibles engendrés par les *cookies* (17), les « Global Unique Identifiers » (18) et les hyperliens invisibles (19). Cette face cachée d'Internet autorise le ciblage des internautes et grâce à lui diverses techniques de *cybermarketing* dont l'efficacité est chaque jour plus remarquable (20). Ces techniques permettent, à partir d'un ciblage *a priori* de l'internaute, tantôt de lui adresser les bannières publicitaires adéquates, tantôt de sélectionner les pages du site les plus appropriées, tantôt de proposer des prix différents (21), tantôt enfin d'interdire l'accès de tel ou tel site à un internaute *a priori* reconnu comme peu solvable. L'opacité provient également de la multiplication des acteurs dont la localisation (22), l'intervention ou les relations entre eux sont parfois mal connues ou mal mesurées. Ainsi qui connaît le rôle exact des fournisseurs d'accès à Internet, celui des portails et les relations de ceux-ci avec les sites qu'ils hébergent ou renseignent, celui des agents de recherche (23), sans parler du rôle des navigateurs ou *browsers*, dont le « bavardage » (24) s'opère souvent à l'insu des internautes eux-mêmes et en direction d'acteurs non identifiables aisément?

6. — Qu'Internet présente donc pour notre vie privée des risques majeurs est incontestable. Cette constatation induit une relecture des dispositions, voire des principes mêmes de nos législations; ce sera l'objet de notre premier chapitre. Au-delà, elle invite à la reconnaissance de nouveaux droits, dont la présentation constituera le second chapitre. Enfin, nous attirerons l'attention sur la manière dont le marché lui-même pourrait offrir des solutions garantissant une plus grande effectivité de la protection de la vie privée.

1 POUR UNE RELECTURE DES DISPOSITIONS ET PRINCIPES DE LA PROTECTION DE LA VIE PRIVÉE

7. — L'irruption d'Internet est récente. C'est dire que les directives européennes et les diverses transpositions nationales de celles-ci n'ont pu prendre en compte ce donné nouveau et les risques associés à son utilisation. C'est donc à un travail soit d'interprétation qu'il faut se livrer pour analyser la manière dont les principes et définitions des directives peuvent trouver application, soit de création dans la mesure où les principes retenus sous l'empire des directives s'avèrent incapables d'offrir une solution satisfaisante. Ce travail — qui ne pourra être que partiel (25) dans le cadre de la présente étude — s'opérera de la manière sui-

(13) La généralisation attendue de l'utilisation de systèmes de cryptographie, pourtant largement libéralisée, est certes une solution à ce problème. La proposition de directive déjà citée note 6 impose une obligation de sécurité aux fournisseurs de services de communications électroniques accessibles au public, en ce qui concerne la sécurité de leurs services et aux fournisseurs de réseaux publics, en ce qui concerne la sécurité du réseau.

(14) A propos du réseau Echelon, cf. l'article déjà cité note 7.

(15) Ainsi, nous écrivions dans le rapport précité : « Bref, la captation abusive de messages par une personne étrangère risque de remettre en cause la souveraineté des Etats en tant cette fois qu'expression du principe d'indépendance de chaque Etat dans l'ordre international. Que devient l'indépendance d'un Etat, si les secrets de ses administrations, de son gouvernement, de ses entreprises, de ses citoyens peuvent être décryptés en des lieux inconnus au profit de puissances étrangères du seul fait qu'ils pénètrent l'espace aérien... ».

(16) En particulier, J.-M. Dinant, « Electronic threats on personal data and electronic data protection on the Internet - Law and technology Convergence in the Data Protection Field? », *Esprit Project*, Eclip, Deliverable 2.2.3., disponible au site Eclip, *www.eclip.or*, en particulier le chapitre 1 : Some Privacy killing slides of the Internet Technology et l'abondante littérature y citée. Du même auteur, « Le visiteur visité - Quand les éditeurs de logiciel passent subrepticement à travers les mailles du filet juridique », *Lex electronica*, vol. 6, n° 2 2001 (disponible sur le site : *www.lex-electronica.org/articles/v6-2/dinant.htm.*). Cf. également le rapport de l'Internet Task Force du groupe dit de l'article 29, présidé par P. Hustinx; « Privacy and the Internet : An integrated E.U. Approach to on-line Data Protection » disponible sur le site *http ://europea.eu.int/Comm/internal_market/eu/media/dataport/wpdocs/wp37en.pdf*.
Le groupe de l'article 29 (par référence à l'article de la directive 95/46 qui le crée) rassemble les représentants des autorités de contrôle en matière de protection des données de l'Union européenne. Le rapport décrit l'ensemble des techniques et services utilisés par les divers acteurs d'Internet et les risques encourus pour la protection des données.

(17) A propos des *cookies*, parmi une littérature riche, lire l'étude effectuée pour le compte de l'O.C.D.E., *Pratiques relatives à la mise en œuvre sur les réseaux mondiaux des lignes directrices de l'O.C.D.E. sur la vie privée* (Doc. « DSTI/ICCP/REG(98)6/final » disponible sur le site de l'O.C.D.E. : *www.ocde.org/dsti/sti/it/secur/act/privnot.htm*., D. Whalen, « The Unofficial Cookie FAQ », disponible à *www.cookiecentral.com/faq*. et l'article de V. Mayer-Schönberger, « The Internet and Privacy legislation : Cookies for a treat? », disponible à *www.wjolt.wvu.edu/wvljolt/current/issue1:articles/mayer/mayer.htm.* et publié *in* 14, *Computer Law and Security Report*, (1998), n° 23, pp. 166 et s.

(18) Sur ce système développé par Microsoft et installé sur les logiciels les plus courants (Excel, Word, Powerpoint), sur le P.S.N. (Processor Serial Number) mis au point par Intel et donnant à chaque unité centrale des processeurs commercialisés par cette firme un numéro de série unique, autant de systèmes qui permettent d'identifier l'origine des transactions opérées à partir de ces systèmes, lire J.-M. Dinant, *Eclip Report,* pp. 2 et s. Cf. égal. comme autre système de traitement invisible, le mouchard électronique intégré dans le lecteur audio de RealjukeBox de la Real Networks Cy qui permet de connaître à distance votre consommation musicale et de repérer le cas échéant des copies illégales en format MP 3 : l'article paru dans *Expertises*, janvier 2000, p. 406.

(19) Sur les hyperliens invisibles, lire J.-M. Dinant, « Les traitements invisibles sur Internet », disponible sur le site du C.R.I.D. (*www.droit.fundp.ac.be/crid/eclip/Luxembourg.htm.*).

(20) Sur ces techniques, l'étude Arete soumise à la Commission européenne, S. Gauthronet, F. Nathan, *Les services en ligne et la protection des données et de la vie privée*, décembre 1998, disponible sur le site de la Commission : *http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm.*

(21) Sur ces techniques de *dynamic pricing*, opérées par Amazon, lire F. de Villenfagne et J.-M. Dinant, « A propos du projet de loi n° 213 », à paraître p. 16 qui cite l'enquête publiée notamment par *Libération* le 28 septembre 2000.

(22) « How can one know to which country such existing adresses correspond : *105473.8880@compuserve.com* or *http://www.telepathic.com.*? And indeed how could a person from Taïwan know whether the town of Gävle mentioned as the point of location of an information provider is situated in Sweden or in Estonia? » (C. de Terwangne et S. Louveaux, *Data protection and on-line Networks*, M.M.R., 1998, pp. 451 et s.).

(23) Sur ces relations, lire outre l'étude Arete, l'article de E. Barchechath, « Une lecture critique du One-to-One », *in Commerce électronique, marketing et libertés*, *Cahier Laser*, n° 2, Paris, Ed. 00h00, 2000, disponible sur le site *http://www.00h00.com.*

(24) « Le bavardage des programmes de navigation constitue une deuxième caractéristique apparaissant comme davantage " privaticide ". Lorsqu'un programme de navigation demande une page à un site Internet, il communique de manière cachée et systématique certaines informations relatives à la machine du demandeur et notamment : le type de système d'exploitation de la machine; le type et la langue du programme de navigation; le type de processeur; la langue parlée par l'internaute; la page référente (c'est-à-dire l'U.R.L. de la page visitée avant la page précédente) ». J.-M. Dinant, *Le visiteur visité*, art. cité, n° 34.

(25) Pour des analyses plus complètes, cf. en particulier le *deliverable* de S. Louveaux, « Internet and Privacy », rapport Eclip, disponible sur le site

vante. Premièrement, on s'intéressera aux définitions relatives à l'objet de la protection. Deuxièmement, on s'interrogera sur les conditions de légitimité des traitements, en particulier la notion de consentement. Enfin, on abordera la question particulière des flux transfrontières.

A. — **Les définitions**

8. — Sans doute, une des questions les plus controversées est celle de l'extension de la notion de donnée à caractère personnel aux données créées par les *cookies*. Cette question abordée par la doctrine récente (26) part de la constatation que les *cookies* créent au profit de ceux qui les émettent et les transfèrent sur le disque dur de l'internaute des informations qui permettront l'identification non de la personne mais de l'ordinateur utilisé par l'internaute qui, chaque fois qu'il sera à nouveau connecté au site émetteur du *cookie*, pourra le reconnaître (27). Or, la notion de donnée à caractère personnel est définie par la directive (28) comme « toute information relative à une personne physique identifiée ou identifiable ». Faut-il sur cette base exclure les données engendrées par des *cookies* du champ de la protection des lois sur la vie privée au motif qu'elle n'identifie qu'un système informatique? L'article déjà cité estime qu'est identifiable une personne qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » et le considérant n° 26 de la directive estime que pour examiner ce caractère identifiable, il faut considérer l'ensemble des éléments susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par un tiers. Cette prise en considération doit-elle se faire *in abstracto* ou *in concreto*? La question n'est pas tranchée par le droit européen. Elle est d'importance dans le cas qui nous occupe, dans la mesure où les sociétés qui pratiquent les *cookies* affirment généralement s'abstenir de toute recherche de l'identité de la personne physique (29) et dès lors seraient considérées comme ne traitant pas des données à caractère personnel, sauf à considérer que le nombre de données engendrées permet de dresser un profil de l'utilisateur révélant psychologiquement sa personnalité (30). L'interprétation retenue en Belgique plaide par contre pour une interprétation extensive : « dès qu'il existe *in abstracto* un moyen raisonnable d'identifier la personne concernée, soit dans le chef de la personne responsable, soit dans le chef d'un tiers, il s'agit d'une donnée à caractère personnel » (31). Or, même si elle est théorique, cette possibilité d'identification existe; en effet le *cookie* identifie l'adresse TCP/IP de l'internaute, qui, même si elle varie dans le temps, se rapporte au fournisseur d'accès qui l'a attribuée et peut dès lors identifier l'abonné qui l'a utilisée.

9. — La proposition de directive qu'a introduit récemment la Commission auprès du Parlement (32) a pour but de remplacer la directive 97/66/C.E. concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications dans la mesure où le contexte de la convergence l'impose. Ainsi, alors que la directive de 1997 visait les « services et réseaux de télécommunications », la proposition étend son champ d'application de manière significative en visant l'ensemble des « réseaux et services de communications électroniques » dans la mesure où ils sont accessibles au public (33). Il s'agit en effet de soumettre à un même cadre réglementaire tous les réseaux et services ayant pour objet principal la transmission et le routage des signaux indépendamment de la technologie utilisée (34), qu'il s'agisse de la câblodistribution ou d'Internet. Sont donc visés des services comme la fourniture d'accès ou de services à Internet (35) ou tous les services de *remailing*. Cette extension est importante dans la mesure où elle instaure un régime dérogatoire pour les traitements opérés dans le cadre de ces réseaux, en particulier à propos des données de trafic, notion déjà utilisée par la directive mais que la proposition définit, et des données dites de localisation, notion nouvelle. Qu'en est-il de ces notions et du régime particulier qui leur est proposé?

10. — La notion de données de trafic est, selon la proposition, à entendre comme « toute donnée (36) traitée au cours ou en vue d'une transmission d'une communication dans un réseau de communication électronique ». Ainsi, la donnée d'adressage d'une transmission via Internet tant de l'émetteur que du destinataire, la durée de la communication, les protocoles utilisés, etc. sont désormais visés (37). De telles

Eclip déjà cité. L'auteur y envisage systématiquement l'application de chaque disposition de la directive dans le contexte d'Internet.

(26) Cf en particulier, les études de V. Mayer-Schönenberg, article cité, p. 168; M.-H. Boulanger et C. de Terwangne, « Internet et le respect de la vie privée », *in* « Internet face au droit », *Cahiers du C.R.I.D.*, n° 12, Namur, Story-Scientia, 1997, pp. 189 à 213; S. Louveaux, *Le commerce électronique et la vie privée*, 10e journée de l'A.B.J.E., 22 oct. 1999, *Le droit des affaires en évolution*, Bruylant-Kluwer, 1999, pp. 183 et s.

(27) ... directement ou à travers un hyperlien (cf *supra*, note 19 sur la pratique des hyperliens par les sociétés de *cybermarketing*).

(28) Article 2.1 de la directive. La définition est reprise par l'article 1er, § 1er, de la loi du 8 décembre 1992 modifiée par la loi du 11 décembre 1998.

(29) On peut légitimement douter de cette assertion dans le cas de société comme Double Click dans la mesure où le rachat par cette société de la société Abacus, société de vente à correspondance, ne peut s'expliquer que par la volonté de lier les données révélées par les *cookies* avec celles utilisées par le commerce à distance traditionnel (sur cette fusion des deux sociétés et ses conséquences en matière de vie privée, lire T. Léonard, *op. cit.*, Coll. V.U.B., n° 6).

(30) ... ce qui sera le cas lorsque des sociétés, en particulier de *cybermarketing,* pourront croiser des informations engendrées par l'utilisation de plusieurs sites.

(31) Cf. Exposé des motifs, *Doc. parl.*, Ch. représ., sess. ord. 1997-1998, n° 1586/1, p. 12. Sur ce point, S. Louveaux, article cité, p. 192. Cette interprétation extensive a conduit le Roi à devoir prévoir en exécution de la loi une réglementation de l'utilisation de toutes les données codées même si ces données sont codées par un tiers (A.R. portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, articles 7 et s. Cet arrêté royal est en cours de publication). L'article 1 définit la donnée codée comme « la donnée à caractère personnel démunie de tout élément permettant d'identifier la personne et munie d'un code qui seul permet de relier la donnée à la personne concernée ».

(32) Cf. les références de cette proposition de directive, *supra* note 6.

(33) Cet ajout prévu par l'article 3 de la proposition de directive a pour effet d'exclure tous les services liés à des intranets, en particulier dans des entreprises. Les dispositions de la future directive ne pourront donc être invoquées par exemple par un employé contre son employeur qui aurait utilisé des données de trafic sans respecter les conditions prévues par la future directive.

(34) La proposition de directive pour un cadre réglementaire commun pour les réseaux et services de communications électroniques (publiée au *J.O.C.E.*, 19 déc. 2000, C 365 E/198 et s.) dans lequel s'insère la proposition de directive spécifique relative à la protection de la vie privée définit le service de communications électroniques comme « le service offert normalement contre rémunération qui consiste totalement ou partiellement en la transmission ou le routage de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et de transmission dans des réseaux utilisés pour la télévision mais en excluant les services fournissant ou exerçant un contrôle éditorial sur du contenu transmis par ces réseaux ou services de communications électroniques » (art. 2, *b*).

(35) Cette extension contestable dans le cadre de la directive de 1997 avait déjà été souhaitée par le groupe de l'article 29, recommandation n° 3/99 (W.P.25) : « Implementation of directive 97/66/E.C. with respect to Internet services » (disponible à l'adresse : *http://europa.eu.int/comm/dg15/en/media/dataprot/WPdocs/htm.*). Cette extension de la directive 97/66 aux services électroniques était implicite depuis l'adoption de la directive du 4 juin 2000 sur certains aspects juridiques du commerce électronique qui se réfère explicitement à la directive 97/66 comme couvrant certains services de la société de l'information. En Belgique, dans le cadre de l'adoption des arrêtés d'exécution de la loi du 21 mars 1991 relative à certaines entreprises publiques (20 avril 1999 et 11 juin 1999, *M.B.*, 21 juill. 1999), le Roi avait étendu la notion de services de télécommunications explicitement aux services d'accès à Internet et soumis ceux-ci aux dispositions transposant la directive 97/66. Sur ce point, lire Th. Léonard, « E-commerce et protection des données à caractère personnel », colloque V.U.B., nos 22 et s.

(36) On rappellera que la directive de 1997 protégeait aussi bien les données concernant les personnes physiques que morales. La proposition de directive ne modifie pas ce choix même si elle introduit, dans certains cas, une distinction entre la protection de l'abonné qui peut être une personne morale et celle de l'utilisateur qui est la personne physique utilisant effectivement les services de l'abonnement. Cette distinction est importante comme il sera noté plus loin en particulier dans le contexte des relations employeurs - employés.

(37) La directive de 1997 faisait référence à des données relatives à des « appels », terme qui dans son sens strict ne pouvait viser que les services téléphoniques transmis par des réseaux à commutation de circuits. Cette limitation est jugée par la Commission comme contraire au principe de « neutralité technologique » qui exige que toute transmission soit visée, peu importe la technologie choisie (transmission par paquets, utilisation d'Internet).

données doivent, édicte l'article 6 de la proposition, être « effacées ou rendues anonymes dès l'achèvement de la transmission ». Trois exceptions sont toutefois prévues : premièrement, le traitement des données nécessaires à l'établissement de la facturation (38); deuxièmement, moyennant à la fois, premièrement, information de l'abonné quant au type de données traitées et à la durée de conservation et, deuxièmement, le consentement (39) de celui-ci, le traitement en vue de la commercialisation de services à valeur ajoutée proposés par le fournisseur du service visé (40); troisièmement, la communication exigée par des autorités compétentes en vue de régler des litiges (41).

Les données de localisation sont définies (42) comme « les données traitées dans un réseau de télécommunications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public » (43). On connaît la précision des données de localisation attachées à la détention et à l'utilisation d'équipements terminaux mobiles et l'offre de services à valeur ajoutée offerts par certains opérateurs, services liés à cette possibilité de localisation (ainsi, dans le cadre de transporteurs routiers ou de service de guidage pour conducteurs). La proposition de directive interdit le traitement des données créées dans le cadre de cette offre de services à valeur ajoutée sans consentement de l'utilisateur ou de l'abonné au service (44) et en toute hypothèse le limite à la durée de ce service. On ajoute que les utilisateurs ou (45) abonnés qui ont consenti gardent en outre la possibilité de désactiver le service gratuitement et par un moyen simple. Enfin, la proposition de directive permet aux services reconnus « d'urgence » la possibilité de passer outre ce consentement ou cette interdiction temporaire (46).

B. — **La légitimité des traitements**

11. — Le principe de légitimité des traitements affirmé par les articles 4 et 5 de la loi du 8 décembre 1992 contient de multiples facettes (47). Il s'agira tantôt du principe suivant lequel la création d'un traitement et sa mise en œuvre doivent respecter un certain équilibre entre les droits et libertés des personnes concernées et les intérêts publics ou privés légitimes poursuivis par le responsable du traitement. Ce principe de légitimité de l'existence d'un traitement se voit précisé par l'article 5 qui énonce *a priori* certaines conditions nécessaires pour asseoir la légitimité de cette existence : ainsi, notamment, le consentement indubitable de la personne concernée, l'exécution d'un contrat et la réalisation d'un intérêt légitime du responsable du traitement ou d'un tiers à qui communication est faite, supérieur à l'intérêt de la personne concernée. En matière de données sensibles (données médicales, judiciaires ou révélant l'opinion religieuse, philosophique, etc.), les articles 6 et suivants restreignent encore ces conditions *a priori* de légitimité. A cette première facette s'en ajoute une seconde : le principe de compatibilité exige, en cas de traitements dérivés d'un premier traitement (48), que le second traitement mis en place ne heurte pas les prévisions raisonnables de la personne concernée créées dans le cadre du premier traitement. Le principe de légitimité de l'existence du traitement implique enfin que le traitement doive s'opérer de manière loyale (49). On distinguera de ces divers aspects de la légitimité qui touchent à l'existence même du traitement, ceux qui touchent à son contenu. L'article 4 de la loi réclame que les données traitées soient nécessaires à l'exécution du traitement et conservées pour la seule durée de cette nécessité. Parmi ces multiples aspects, seuls certains seront abordés.

12. — L'analyse des dispositions de la proposition de directive en matière de données de trafic et de localisation révèle des dérogations importantes aux principes de légitimité des traitements affirmés par l'article 6 de la directive et repris chez nous à l'article 5 de la loi de 1992. Ainsi, le traitement des données de trafic et de localisation a comme principal et quasi unique fondement le consentement des personnes concernées. Cette restriction du fondement de l'existence des traitements de données à des hypothèses de consentement dans le contexte de l'utilisation d'Internet est remarquable. La même proposition de directive entend soumettre également au consentement de la personne concernée l'envoi de courriers électroniques à des fins de prospection commerciale. En matière d'interception de communications téléphoniques, mais également électroniques (50), l'article 314*bis* du Code pénal interdit, à quiconque n'y prend part, la prise de connaissance, l'interception ou l'écoute de communications ou télécommunications privées, sauf le consentement de tous les participants à ces communications ou télécommunications privées. La dix-septième chambre du tribunal correctionnel de Paris (51) a récemment rappelé ce principe en condamnant un

(38) Dans le cas d'abonnement gratuit ou forfaitaire et non à la communication, ce qui est le cas de la plupart des abonnements proposés par des fournisseurs d'accès à Internet, le nombre de ces données sera singulièrement réduit.

(39) Nous reviendrons sur cette notion, fondement de la légitimité de nombre de traitements sur Internet (*infra*, n° 14).

(40) Ce qui est souvent le cas. Nombre de fournisseurs d'accès proposent des services supplémentaires : hébergement de sites web, services de *news* ou de forums de discussion, services d'anonymat, etc.

(41) ... ce qui exclut, notons-le, le droit des autorités arbitrales, de médiation ou de conciliation privées d'y avoir accès. Autre exception : on ajoutera la communication susceptible d'être exigée par des autorités publiques chargées de la prévention, de la détection et de la poursuite d'infractions pénales, communication prévue par l'article 15 de la proposition de directive. Cette exception soulève, comme le note la Commission de protection de la vie privée dans son avis sur le récent projet de loi sur la criminalité informatique (...), un problème délicat. En effet, dans la mesure où la loi requerra la conservation des données de trafic dans le cas de la lutte contre le cybercrime, elle justifiera toujours une conservation des données par les fournisseurs d'accès, conservation qui par ailleurs leur est souvent proscrite par les dispositions rappelées. Nous reviendrons sur cette question à propos du droit à l'anonymat (*infra*, n^os 23 et s.).

(42) Article 2, *c*, de la proposition de directive.

(43) On notera à la suite du préambule de la proposition de directive que certaines données sont à la fois des données de localisation et des données de trafic dans la mesure où la localisation même imprécise du terminal est nécessaire pour acheminer la transmission du message.

(44) Ce consentement sera préalablement informé quant au type de données de localisation traitées, aux objectifs et à la durée du traitement et, le cas échéant, des transmissions à des tiers dans le cadre du service offert.

(45) Le « ou » soulève des questions délicates d'interprétation dans la mesure où l'utilisateur ne s'identifie pas à l'abonné (cf. note n° 36). Le cas le plus fréquent est celui de l'employé disposant d'un terminal mobile et de services souscrits par son employeur. Faudra-t-il dans ce cas informer l'employé *ET* l'employeur et obtenir leur double consentement? Comment le fournisseur devra-t-il procéder s'il faut ce double consentement? L'utilisateur qui aurait consenti peut-il désactiver temporairement la localisation du terminal en toute hypothèse ou seulement dans les limites prévues par le contrat de travail?

(46) De même pour les autorités publiques chargées de la prévention, de la détection et de la poursuite d'infractions pénales (*supra*, note 41).

(47) Sur ces multiples facettes, T. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *in* F. Rigaux, *La vie privée : une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, n° 17, Larcier, 1992, pp. 250 et s.; S. Gutwirth, « De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijk levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993, pp. 1409 et s.

(48) Ex., le responsable du traitement collecte des données pour une finalité d'exécution des transactions conclues avec la personne concernée et décide à un moment donné d'utiliser les données engendrées par le premier traitement à des fins de ciblage de clientèle et de prospection commerciale, voire de commercialiser de telles données.

(49) ... ce qui condamne les traitements opérés à partir de techniques de collecte non transparente comme c'est le cas dans les traitements dits invisibles décrits plus haut (*supra*, n° 5).

(50) L'exposé des motifs de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (*Doc. parl.*, Sénat, sess. ord., 1992-1993, n° 843-1, p. 7) affirme explicitement que la loi vise « la transmission électronique de données dans des ordinateurs ou des réseaux d'ordinateurs ». La doctrine est unanime à cet égard (cf. pour une revue de la littérature, P. Lambert, « Bescherming van prive-(tele)communicatie - Recente ontwikkelingen in informatica- en telecommunicatierecht », *I.C.R.I.*, Brugge, Die Keure, 1999, pp. 185 et 193). A noter dans le même sens d'une interprétation extensive, la recommandation 2/99 du groupe de l'article 29 concernant le respect de la vie privée dans le contexte de l'interception des communications privées du 3 mai 1999 (disponible à l'adresse : *http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm*) à propos de la résolution du Conseil relative à l'interception des télécommunications (publié *in J.O.*, C 329, 14 nov. 1996).

(51) Corr. Paris, 2 nov. 2000, texte disponible au site : *www.droit-technologie.org/fr/4 1.asp?jurisprudence id=4*.

laboratoire de recherche qui avait exclu un étudiant après avoir pris connaissance de l'existence d'*e-mails* ou courriers personnels.

Cette dernière disposition pénale reçoit un champ d'application extrêmement large dans le contexte d'Internet puisqu'elle permettrait de suspendre au consentement de l'internaute, les surveillances opérées par l'employeur de l'utilisation d'Internet par ses employés (52) et les transferts automatiques lors de visites de sites, transferts opérés par des hyperliens (53). Sur ce dernier point ne peut-on en effet, à la suite de M. Léonard (54), considérer que « la simple visite d'un site et, *a fortiori*, toute expression d'une interactivité entre un site et un internaute — par exemple lors de la rédaction d'un bon de commande d'un produit ou service par un internaute et son renvoi vers le site ou lors de l'envoi des informations relatives à un paiement — sont constitutives de communications et/ou de télécommunications privées entre le prestataire de service et l'internaute? Ne faut-il pas également qu'il en soit de même concernant les informations issues de l'utilisation des protocoles techniques utilisés et du bavardage des logiciels de navigation?... Tout tiers qui viendrait enregistrer ces informations lors de leur transmission agirait donc en violation de l'article précité s'il n'obtenait pas le consentement des parties ». Ce raisonnement condamne bien évidemment la pratique de certaines sociétés de *cybermarketing* opérant par hyperliens invisibles et obligerait à suspendre le déclenchement de l'hyperlien à un consentement informé de l'internaute, celui-ci fût-il obtenu par un simple clic.

13. — Enfin, la même proposition de directive suspend au consentement préalable du destinataire potentiel l'envoi de communications commerciales par courrier électronique : « L'utilisation de systèmes automatisés d'appel sans intervention humaine, de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable » (55).

14. — Deux justifications paraissent pouvoir fonder cette omniprésence du consentement comme base quasi exclusive de légitimité des traitements sur Internet. La première est certes le fait que les risques liés à la multiplication possible des traitements à partir des données engendrées par l'utilisation d'Internet, réseau ouvert, opaque et global, justifie qu'on restreigne les causes de légitimation des traitements et notamment qu'on écarte l'application de l'article 7, *f*, de la directive (56) qui autorise le traitement si les intérêts à traiter les données avancées par le responsable ou le tiers auquel on communique sont supérieurs à l'intérêt de la personne concernée à la confidentialité. Une telle balance est difficile à opérer et supposerait la possibilité effective de la personne concernée de connaître tous les traitements opérés et de faire valoir ses intérêts, ce qui peut parfois être difficile vu le caractère global du réseau. L'autre explication tient au caractère interactif du réseau qui permet de donner au consentement sa pleine efficacité. C'est en effet la personne concernée qui, par l'utilisation de son équipement est l'auteur des données créées. Pourquoi ne pas lui permettre de décider si oui ou non elle souhaite recevoir des *cookies*, s'identifier, voir ses données transmises à un tiers, recevoir ou non des courriers publicitaires, etc. (57)? Le consentement permet au consommateur de décider si oui ou non il accepte de céder, le cas échéant contre monnaie sonnante et trébuchante, ses données personnelles (58).

15. — Ceci dit, de quel consentement parle-t-on et celui-ci légitime-t-il tout traitement? On rappellera à la suite de l'article 1er, § 8, de la loi belge (59) que le consentement doit être libre (60), spécifique et informé (61). On ajoutera que le consentement est certes une condition de licéité du traitement, mais non une condition suffisante (62). « La loi nouvelle dispose certes que le consentement suffit pour légitimer un traitement, fût-il de *marketing one-to-one.* Cette possibilité de légitimation n'est cependant pas absolue. Le jeu des articles 4 et 5 de la loi impose, selon nous, de considérer que la condition de légitimité, présente à l'article 4, l'emporte sur les conditions de légitimité posées *a priori* par l'article 5 de la même loi. L'article 4 joue comme un garde-fou qui peut trouver à s'appliquer dans la problématique à analyser. Le consentement donné dans le cadre de l'application de la loi implique une condition particulière : l'atteinte librement consentie ne peut pas être disproportionnée » (63). Par ailleurs, le consentement ne peut mettre en cause la dignité humaine (64). Ainsi, le consentement portant sur des données intimes de la personne concernée qui souscrirait à la possibilité

(52) La recommandation de la Commission belge de protection de la vie privée n° 10/2000 du 3 avril 2000 se montre sur ce point réservée tant est évidente une certaine légitimité du contrôle par les employeurs de l'utilisation de leur outil de travail. (...). La question pour la Commission belge est celle de la proportionnalité des moyens de contrôle utilisés par rapport aux risques encourus par l'employeur. Ainsi, un contrôle du contenu des *mails* envoyés n'est pas nécessaire *a priori* et des logiciels de filtrage peuvent réduire les utilisations illégitimes des employés de leur outil de travail. Aux Etats-Unis et au Canada, il est clairement plaidé que l'employé n'a pas d'« expectative raisonnable de vie privée » en ce qui concerne leur courriel. Sur ce point lire H.-L. Rasky, « Can an employer search the contents of his employees e-mail? » (1998) 20 *Advocates'Q.,* pp. 221 et s., ainsi que la jurisprudence y citée.

(53) Sur ce point, les réflexions de V. de Villenfagne et de J.-M. Dinant, art. cité, à paraître, nos 30 et s.

(54) Th. Léonard, art. cité, colloque V.U.B., 2000.

(55) Cette disposition de l'article 13, alinéa 1er, met fin à une incertitude née de la multiplication de dispositions européennes en matière de communications non sollicitées ayant des portées et des solutions parfois contradictoires (sur tout cela le rapport à la C.N.I.L. de Mme C. Alvergnat, *Electronic Mailing and Data Protection*, 14 oct. 1999, disponible sur le site de la C.N.I.L. (*www.cnil.org*). L'alinéa 2 de l'article 13 laisse aux Etats membres le choix en ce qui concerne les communications non sollicitées, effectuées à des fins de prospection commerciale par d'autres moyens (ainsi, les bannières publicitaires, les messages interstitiels, etc.).

(56) ... ou article 5, *f*, de notre loi.

(57) Sur cette « contractualisation » de la *privacy*, vue comme la solution à la question de la protection des données, voy. l'article de Bibas, « A contractual approach to Data Privacy », *Harvard Journal of Law and Policy*, (1994), pp. 591 et s. Nous reviendrons *infra* no 28 sur la manière dont techniquement, le protocole P3P entend permettre une réalisation effective de ces divers objets du consentement.

(58) Au terme, la donnée personnelle devient ainsi un bien, susceptible de transaction commerciale. Sur cette tendance en particulier de la doctrine américaine à considérer la *privacy* comme une *commodity*, objet possible de transaction, lire la remarquable étude de A. Pierrucci, « Contractual Autonomy and the role of consent in the E.C. Directive on Privacy and Telecommunications », *in Legal Issues of the Information Society*, 20-21 July 2000, Maastricht, à paraître.

(59) Qui reprend les exigences de la directive (art. 2, *h*). Sur ces trois exigences et leur interprétation dans le contexte d'Internet, lire Th. Léonard, « E-commerce et protection des données à caractère personnel », art. cité, colloque V.U.B., nos 8 et s.

(60) Ce qui peut parfois être remis en question. Ainsi, lorsque l'acceptation de *cookie* est la condition nécessaire pour l'entrée dans un site ou lorsque la délivrance d'informations préalables est une condition de l'offre d'un service gratuit d'accès à Internet.

(61) La recommandation no R (99)5 du Conseil de l'Europe estime que l'information doit couvrir non seulement les caractéristiques du traitement (personne responsable, finalités poursuivies, droit d'accès,...) mais aussi les risques liés à l'utilisation d'Internet (ainsi, la faible sécurité du réseau, les modes de collecte invisibles...). Une interprétation de l'article 9 de la loi belge pourrait conduire à cette même conclusion dans la mesure où l'article prévoit l'obligation d'informations supplémentaires « déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la Commission de protection de la vie privée ».

(62) Pour un même raisonnement à propos des articles 6 et 7 de la directive, lire M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau, Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, p. 146. Pour le raisonnement en droit belge, T. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, pp. 384 et 385, no 27 et les références à l'exposé des motifs de la loi; A. Pipers et P. de Hert, « Handboek *Privacy*-persoonsgegevens in België », *Politeia*, 1999, p. 65.

(63) A. Pierucci, art. cité, p. 24; T. Léonard, art. cité, colloque V.U.B., no 17.

(64) Sur les limites à la contractualisation imposées par le respect de la « dignité » humaine, lire dans le domaine de la biomédecine, M.-Th. Meulders-Klein, « Biomédecine, famille et droits de l'homme : une même éthique pour tous? » *Rev. trim. dr. h.*, 2000, p. 437 : « Sur le continent au contraire, du moins traditionnellement, la dignité de l'homme justifie qu'il ne puisse se nuire volontairement à lui-même, et indirectement à la société, fût-ce au nom de sa liberté. Il y a donc une tension entre liberté et protection de la personne que ne connaît pas le droit anglais, outre le fait que si le but poursuivi est jugé immoral, le consentement lui-même ne serait pas valable. Si celui-ci est donc nécessaire, il n'est pas suffisant ». Même réflexion *in* M.-L. Pavia, « Le principe de dignité de la personne humaine : un nouveau principe constitutionnel », *in Droits et libertés fondamentaux*, Dalloz, Paris, 4e éd., 1996, pp. 99 et s.

d'un traitement infamant (65) heurterait les droits fondamentaux de la personne et serait contraire à l'ordre public. Enfin, comme le notent A. Pierucci et T. Léonard (66), doivent s'appliquer à de tels consentements, les enseignements de la théorie générale des contrats tant sur le vice de consentement (67) que sur le caractère lésionnaire d'une transaction où, en échange d'un vil avantage ou prix, un opérateur obtiendra des informations dont la valeur est de loin supérieure.

16. — Le principe de compatibilité suivant lequel les données ne peuvent « être traitées ultérieurement de manière incompatible avec ces finalités (celles de la collecte), compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé... » (68) trouve dans le cadre d'Internet des applications utiles. La Commission de protection de la vie privée, dans un tout récent avis d'initiative (69), notait en ce sens : « Les données communiquées par un acheteur, par exemple dans le cadre d'une transaction, ne peuvent ainsi être réutilisées et transmises par le vendeur à un tiers (une société de crédit, une compagnie d'assurances) qui serait intéressé par le profil des clients. En ce qui concerne la collecte des adresses de courrier électronique sur des sites publics tels que des forums, des groupes de discussions (généralement désignés par le terme *chat*), annuaires ou listes de diffusion, le principe de compatibilité a pour conséquence que ces adresses, qui sont diffusées dans un contexte bien spécifique, ne peuvent pas être collectées et réutilisées à des fins de prospection » (70).

17. — Enfin sur le plan du contenu des traitements, les facilités qu'offre Internet dans la collecte des données, du fait en particulier du caractère interactif du réseau, expliquent l'abondance souvent injustifiée des données réclamées ou traitées par rapport à la finalité légitime poursuivie par le responsable du traitement. L'exemple des traitements opérés dans le cadre de la surveillance des employés peut être cité ici : ce qui est mis en cause par la Commission belge de protection de la vie privée (71) n'est pas la légitimité de l'existence d'un traitement mais la possible disproportion de son contenu. Le contrôle de l'activité d'un employé ne nécessite pas la collecte du détail de l'ensemble des utilisations effectuées par ce dernier de son outil informatique mais bien de seuls indicateurs plus globaux (temps passé sur l'ordinateur, type de services utilisés, etc.). Autre exemple, dans l'étude O.C.D.E. déjà mentionnée relative aux sites de commerce électronique (72), on relève que dans près des deux tiers des sites certaines des informations demandées à travers les formulaires d'inscription, les formulaires *feed-back* et surtout à travers les questionnaires, sont facultatives... Parmi les données facultatives, on trouve assez souvent l'adresse *e-mail* et le numéro de téléphone, l'âge, le sexe, la profession, certaines préférences et habitudes personnelles; dans quelques cas, la fourniture de réponses aux questions facultatives permet aux visiteurs d'acquérir en échange des points-cadeaux; dans un autre cas, de participer à un concours...

C. — **Les flux transfrontières**

18. — Le caractère global du réseau des réseaux : Internet et surtout le fait que plus de 80% des sites sont encore à l'heure actuelle nord-américains et que le trafic européen Internet est acheminé sur des réseaux non européens justifient la préoccupation des autorités face à la multiplication des flux transfrontières. On connaît sur ce thème les dispositions de la loi belge paraphrasant d'ailleurs la directive. Elles sont d'ordre divers : la première est celle de l'article 3*bis*, 2°, qui soumet à la loi belge le responsable non établi en Belgique qui recourt à des fins de traitement « à des moyens automatisés localisés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit ». Les dispositions des articles 21 et suivants édictent le principe suivant lequel « le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non-membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat » mais prévoient des exceptions à cette interdiction de principe soit dans certains cas de flux légitimés de manière spécifique (73), soit lorsque des dispositions contractuelles présentent des garanties suffisantes. A propos de ces dispositions, sans prétendre être exhaustif, trois questions seront abordées : la première porte sur le champ d'application respectif des différentes dispositions; la deuxième, sur la question de l'application de l'article 21 à des collectes de données directement créées par l'internaute; la troisième commente brièvement les règles contenues dans les « Safe Harbor Principles », document signé entre la Commission européenne et le « Department of Commerce » américain qui détermine les conditions du caractère adéquat de la protection offerte par les entreprises américaines.

19. — A propos du champ d'application de l'article 4 de la directive que reproduit imparfaitement la disposition belge de l'article 3*bis*, la doctrine (74) s'est ralliée aux conclusions de l'étude de M. H. Boulanger et C. de Terwangne (75) qui considéraient que cette disposition trouvait application dans des cas bien circonscrits pour les flux passifs, c'est-à-

(65) Certes, cette exception sera rare dans la mesure où il est acquis que la contractualisation des biens de la personnalité est possible. A cet égard, les références de T. Léonard (*eod. loc.*) et notamment aux conclusions de P. Keyser : « Le contrat consiste en effet dans l'acceptation, par une personne, de la proposition d'une autre de s'immiscer dans sa vie privée ou de la divulguer, de réaliser ou de publier son image ». Cf. la conclusion dans le même sens de F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruxelles-Paris, 1990, p. 763. « Dans une société qui forme un marché d'échange généralisé, il n'est guère de biens de la personnalité qui ne puissent, avec le consentement du sujet, se transformer en valeur marchande ».

(66) Cf. les articles déjà cités note 62.

(67) A. Pierucci (p. 27) cite notamment le droit du consommateur d'invoquer la « misrepresentation » créée par une publicité trompeuse ou déloyale.

(68) Le critère des prévisions raisonnables de l'intéressé *(legitimate expectation of privacy)* est le critère retenu par le législateur belge pour définir la compatibilité ou non d'un traitement.

(69) C.P.V.P., avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique, avis n° 34/2000 du 22 novembre 2000.

(70) On peut suggérer d'autres applications du principe : ainsi, certains moteurs de recherche puissants permettent par le scannage des sites web de retrouver d'intéressantes similarités entre des personnes ayant publié sur un même thème. On peut songer par exemple à tous ceux qui ont pris partie dans une affaire par des écrits engagés. Ce type d'utilisation des moteurs de recherche est incompatible avec la finalité de la publication sur site web par l'auteur de l'écrit. Le Data Protection Registrar a suggéré récemment la possibilité pour les détenteurs de sites web de disposer d'un sigle « no robot » qui interdirait la recherche par « search engines » (sur ces différents points, lire le « Report and Recommendations » de l'International Working Group on data protection in telecommunications, « Data protection and search engines on the Internet », 14-15 avril 1998, disponible au site : *www.datenschutz-berlin.de*. Autre exemple : la publication des décisions juridictionnelles sur Internet exige que les décisions soient publiées sans référence au nom des parties sans quoi l'utilisation de moteurs de recherche permettra à toute personne ayant accès à la base de données de connaître rapidement le passé judiciaire d'un individu, ce qui certes n'est pas le but de la publication et apparaît à tout le moins comme incompatible avec cette finalité (sur ce second cas, lire Y. Poullet, « Autour de l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'Etat », *in La pathologie législative, comment en sortir?*, Bruxelles, Coll. Droit en mouvement, 1998, pp. 55 et s. et surtout la thèse de Cécile de Terwangne, « La mission publique d'information dans le contexte de la société de l'information », thèse présentée à Namur le 24 nov. 2000, nos 580 et s., thèse à paraître.

(71) Avis n° 10/2000 du 3 avril 2000 déjà cité note 8.

(72) Groupe d'experts sur la sécurité de l'information et la vie privée, Projet d'étude sur les instruments et mécanismes relatifs à la mise en œuvre sur les réseaux globaux des lignes directrices de l'O.C.D.E. sur la vie privée, DSTI/ICCP/REG (98) 6, Paris 18 et 19 mai 1998.

(73) ... ainsi, notamment les cas plus courants en matière d'Internet, en cas de consentement indubitable au transfert (art. 22, § 1er, 1°, de la loi) — notons que dans ce cas la personne concernée doit être au courant que le traitement est localisé à l'étranger et doit marquer explicitement son accord sur ce point — ou lorsque le transfert est nécessaire à la conclusion ou à l'exécution du contrat, par exemple lors de transactions passées via Internet qui rendent nécessaires l'envoi de données pour la finalisation ou l'exécution de la commande (adresse de la personne, numéro et carte de crédit...). Sur ces exemples et d'autres, lire S. Louveaux, article cité, colloque A.B.J.E., 1999, pp. 183 et s.

(74) En particulier cette interprétation est confirmée par le groupe dit de l'article 29, « Privacy on the Internet », document de travail, adopté le 21 novembre 2000, p. 27 et par la Commission de protection de la vie privée dans son avis sur le commerce électronique, déjà cité, p. 7.

(75) M.-H. Boulanger et C. de Terwangne, « Internet et le respect de la vie privée », *in* « Internet face au droit », *Cahier du C.R.I.D.*, n° 12, Namur, Story-Scientia, 1997, p. 205.

dire ceux qui se font à l'insu de la personne concernée et pour lesquels c'est l'utilisation à distance de l'équipement de l'internaute qui déclenche la collecte de données; ainsi les traitements créés par les *cookies* ou les puces permettant d'identifier cet équipement comme le *Global Unique Identifier* ou, dans les cas de « web spoofing » où la collecte de données s'opère via un site miroir localisé dans le pays européen, directement à l'étranger. Ainsi dans le cas Yahoo qui a défrayé la chronique récemment, il a été démontré que le site Yahoo.fr servait de simple instrument de collecte sans qu'un traitement local des données n'ait lieu en France (76). Dans ces deux cas, le responsable du traitement localisé à l'étranger utilise bien un équipement situé sur le territoire européen. Dans les autres cas, c'est-à-dire la quasi-totalité des flux actifs, c'est-à-dire ceux faits par la personne concernée, ce sont les dispositions des articles 25 et suivants de la directive, soit l'équivalent de nos articles 21 et suivants qui s'appliqueront.

20. — Certains ont cependant mis en doute l'applicabilité des articles 21 et suivants aux cas fréquents où l'internaute est en contact direct avec un site étranger au motif que l'article 3*bis* de notre loi belge, qui fixe le champ d'application matériel de la loi, ne permet l'application de la loi belge que soit dans le cas d'un traitement effectué dans le cadre des activités réelles et effectives d'un établissement fixe situé en Belgique ou dans l'hypothèse visée plus haut de l'utilisation de moyens automatisés ou non situés sur le territoire belge. La première hypothèse ne serait pas applicable dans la mesure où, en l'occurrence, les données engendrées par la visite d'un site ne constituent pas, en Europe du moins, un traitement. Dès lors les flux transfrontières de telles données soit ne seraient pas visés par la loi belge, soit devraient nécessairement tomber dans la seconde hypothèse, et le responsable du site visité situé à l'étranger se verrait alors appliquer la loi belge. Cette interprétation ne nous paraît pas devoir être suivie dans la mesure où la directive 95/46, dont la loi belge assure la transposition, donne aux Etats une compétence particulière en matière de flux transfrontières, que les données exportées aient fait en Europe l'objet d'un traitement ou non : « Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert... ». L'article 4 de la directive (77) dont s'inspire notre article 3*bis* n'a pas pour but de déterminer le champ d'application matériel de la directive mais plutôt de fixer la loi applicable en matière de traitements. En d'autres termes, la disposition contenue dans l'article 3*bis* ne peut être interprétée dans le sens indiqué ci-dessus et l'article 21 doit pouvoir s'appliquer (78).

21. — Si les articles 21 et suivants s'appliquent dans la plupart des flux transfrontières effectués par Internet, la détermination du caractère adéquat de la protection offerte par le pays étranger est alors à résoudre. La Commission européenne vient, en fonction des compétences qui sont les siennes (79), de considérer que les « Safe Harbor Principles », mis en place par le « Department of commerce » américain (80) et auxquels les entreprises américaines doivent librement souscrire, constituaient la protection adéquate requise par la directive. Ce n'est pas le lieu de se livrer à une analyse détaillée de ces principes ni à une critique de la décision de la Commission (81) au regard des principes que le groupe de l'article 29 avait lui-même mis en place (82) mais simplement d'en résumer les grandes lignes.

L'accord repose sur six principes de base : celui de l'information de la personne concernée, des restrictions au transfert, de la sécurité, de l'intégrité des données, de l'accès de la personne et de l'effectivité des principes. Sur ce dernier point, on souligne que le bénéfice de la protection adéquate suppose la déclaration du respect des principes au département du commerce, accompagnée d'un certain nombre d'informations sur les activités de l'entreprise. Enfin, les mécanismes de contrôle et de respect mis en place par les « Safe Harbor » reposent, dans un premier temps, sur l'existence de mécanismes de recours auprès d'autorités privées indépendantes, dans un second temps, sur la possibilité d'un recours auprès de la « Federal Trade Commission » pour *misrepresentation*.

2 POUR LA RECONNAISSANCE DE NOUVEAUX DROITS

22. — A l'accroissement des risques que représente Internet doit correspondre la reconnaissance de nouveaux droits (83). Quelques textes déjà les consacrent de manière embryonnaire. Notre propos est simplement d'en souligner l'émergence, d'en proposer une formulation et d'en analyser les conséquences. Ainsi, quatre droits semblent s'imposer dans l'environnement nouveau d'Internet : le premier est certes le droit à l'anonymat dont les limites, en particulier au regard des nécessités de la lutte contre le cybercrime, doivent être soigneusement étudiées. Le deuxième est celui du droit à des technologies respectueuses de la vie privée et de ses principes. Le troisième principe consacre la convergence entre les intérêts de l'internaute comme consommateur et comme citoyen soucieux du respect de sa vie privée. Enfin, un quatrième principe dit de la « réciprocité des avantages » exige que dans la même mesure où Internet facilite le traitement de données personnelles, il facilite également l'exercice par l'internaute de ses propres droits.

A. — **Le droit à l'anonymat**

23. — Nombre de textes à portée souvent non contraignante préconisent le droit du citoyen à l'anonymat (84) lorsqu'il utilise les services nouveaux offerts par les technologies nouvelles. La recommandation n° R (99) 5 du comité des ministres du Conseil de l'Europe approuve, parmi les lignes directrices pour la protection des personnes à l'égard de la

(76) Il s'agissait de la réclamation portée par diverses associations françaises contre la société Yahoo qui accueillait sur ses sites d'enchères des objets nazis. Le président du tribunal de grande instance français devait en deux temps (le 22 mai et le 20 novembre) condamner la société « à prendre toutes mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis » (la décision du 20 novembre est disponible sur le site *www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm*).

(77) Comme le titre de l'article l'affirme d'ailleurs : « Droit national applicable ».

(78) Ceci est d'autant plus évident que l'article parle de l'application de la loi à des traitements alors que l'article 21 se réfère à des données faisant l'objet de traitements après leurs transferts et non à des traitements dont certaines données ou toutes feraient l'objet d'une exportation.

(79) L'article 25(6) de la directive 95(46) permet en effet à la Commission européenne de se prononcer sur le caractère adéquat de la protection offerte par un pays tiers (cf. Commission Decision on the adequacy of the protection provided by the Safe Harbor Questions issued by the US Department of Commerce, 26 July 2000 C(2000)2305).

(80) Le texte du Safe Harbor peut être trouvé sur le site du Department of Commerce américain (*www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm*) ou de l'association Epic (*www.epic.org/privacy/intl*).

(81) Sur cette analyse des Safe Harbor et la critique de la position de la Commission européenne, on lira l'analyse de l'auteur : « Les Safe Harbor Principles : une protection adéquate? », *Juriscom.net*, 17 juin 2000, disponible à l'adresse : *www.juriscom.net/uni/doc/20000617.htm*. Cf. également les remarques du Transatlantic Consumer Dialog (une alliance des associations de consommateurs américains et européens) disponible à *www.epic.org/privacy/intl/tacd_sh_1299.html* et celles au Parlement européen : *www.europarl.eu.int/dg3/sdp/brief/en/br000703_ens.htm#9*.

(82) En particulier, le rapport du groupe de l'article 29, « Transferts de données à caractère personnel à des pays tiers application des articles 25 et 26 de la directive européenne relative à la protection des données », doc. adopté le 24 juillet 1998 et disponible sur le site de la Commission européenne déjà mentionné.

(83) L'idée de ces nouveaux droits a été émise en conclusion des travaux du premier *workshop* d'Eclip tenu à Namur, en 1999 (Y. Poullet, *Internet and Privacy : any conclusions*, texte disponible sur le site du C.R.I.D. (*www.droit.fundp.ac.be/crid.htm*). Elle a fait l'objet de développements *in* S. Louveaux, Y. Poullet et A. Salaün, « Recommendations on User Protection », *Info*, n° 1/6, décembre 1999, pp. 521 et s.

(84) Sur ce nouveau droit, lire notamment S. Rodota, « Beyond the E.U. Directive : Directions for the future, in Privacy : New risks and opportunities », Y. Poullet, C. de Terwangne et P. Turner (ed.), *Cahiers du C.R.I.D.*, n° 13, p. 211.

collecte et du traitement de données à caractère personnel sur les « inforoutes » (85), le principe suivant : « L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée ». Le groupe dit de l'article 29, dès 1997, adoptait la recommandation 3/97 intitulée « l'anonymat sur Internet » (86) et préconisait de même la possibilité d'utiliser des pseudonymes et des techniques d'anonymat lors de l'utilisation de services ou de moyens de paiements électroniques sur Internet (87). Plus récemment, la directive du 13 décembre 1999 fixant un cadre communautaire pour les signatures électroniques (88) établit le droit à utiliser un pseudonyme en matière de signature électronique et la proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques permet aux utilisateurs de refuser, ou le cas échéant de bloquer temporairement, le traitement des données de localisation (89). Enfin, la Commission belge de protection de la vie privée, dans un avis récent sur le commerce électronique et la vie privée (90), rappelle à bon escient l'existence de mécanismes qui permettent d'authentifier l'émetteur d'un ordre (être certain qu'il est bien celui qu'il prétend être) sans que pour autant ce dernier n'ait à s'identifier (donner son nom).

24. — Le principe est donc indiscutablement que l'internaute doit avoir le choix de rester anonyme en ligne comme il a le choix de le rester hors ligne (91) et doit avoir gratuitement les moyens de ce choix via des procédés aisés et accessibles à tous. Ce principe peut dans certains cas céder, lorsque des raisons d'intérêt public supérieures l'emportent. Ainsi, reconnaît-on aux autorités policières le droit d'identifier les coupables de certaines infractions et oblige-t-on les fournisseurs de services de communications électroniques à coopérer à cette identification (92). En Belgique, le projet de loi relatif à la criminalité informatique (93) institue de nombreux devoirs de collaboration des opérateurs de services de télécommunications lors de la recherche d'infractions en cas de perquisitions ou d'« écoutes téléphoniques » (94). Un projet de convention internationale (95) est actuellement en discussion au sein du Conseil de l'Europe qui prévoit ce même devoir. Et la proposition de directive déjà mentionnée, si elle reconnaît le droit à l'anonymat et à la non-identification, ajoute en son article 15.1 que les Etats membres peuvent prendre des mesures législatives visant à limiter ces droits « lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de communications électroniques ».

25. — Si la prescription de tels devoirs est légitime pour assurer l'efficacité des poursuites et lutter contre l'opacité des réseaux qu'accroît encore l'utilisation de systèmes d'anonymat et de non-identification, il paraît cependant nécessaire de rappeler les principes mêmes de l'article 8 de la Convention européenne pour limiter les prérogatives policières et le devoir de collaboration des fournisseurs de services de télécommunications. La loi (96) doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte au respect de la vie privée, et d'autant plus précis que « les procédés techniques utilisables ne cessent de se perfectionner » (97). Son intervention doit être strictement proportionnée aux besoins nouveaux de recherche des infractions que justifie la donne nouvelle que constitue l'utilisation des réseaux et des techniques d'anonymat ou de cryptographie (98). Ainsi, à deux reprises, le groupe de l'article 29 a considéré qu'un fournisseur d'accès ne devait pas être contraint à enregistrer et conserver des données de trafic ou, plus largement, de télécommunications concernant ses clients, que dans le cadre d'une instruction ordonnée par rapport à un ou des clients déterminés (99).

B. — **Le principe de la réciprocité des avantages**

26. — Le principe peut s'énoncer comme suit : dans la même mesure où Internet facilite, pour les fournisseurs de services de communications électroniques, la collecte et le traitement des données, ceux-ci doivent permettre à l'utilisateur de profiter du même médium pour l'exercice

(85) Le texte de ces lignes directrices est disponible sur le site du Conseil de l'Europe : *www.coe.fr/dataprotection/rec/flignes.htm*.

(86) ... adoptée le 3 décembre 1997 et disponible sur le site *http://europa.eu.int/comm/dg15/fr/media/wp.docs/index.htm*. A noter également le quatrième commandement retenu par l'International Working Group on Data Protection in Telecommunications lors de la réunion de Berlin du 28 septembre 2000 : « Right to Anonimity : Networks and Service Providers have to offer to any user the option to use the network or to access the services anonymously or using a pseudonym... ».

(87) Sur ces techniques, lire le document de travail « Privacy on the Internet - An integrated Approach to On-line Data Protection », doc. cité, note 16, en particulier, pp. 81 et s. et les références y reprises.

(88) Directive 1999/93/C.E. publiée au *J.O.C.E.*, L. 13/12, du 19 janvier 2000. L'article 8 interdit aux Etats européens la possibilité de s'opposer à l'utilisation de pseudonymes.

(89) Article 9, alinéas 1er et 2. Cet article s'applique clairement aux données engendrées par l'utilisation de réseaux mobilophoniques. L'article 8 permet des restrictions à l'identification de la ligne appelante soit de manière globale, soit ligne par ligne, soit au cas par cas. Il est regrettable que cette restriction ne concerne que les services téléphoniques. On aurait pu souhaiter, sur la base du principe de neutralité technologique prônée par la proposition de directive elle-même, que ce principe de la restriction téléphonique soit étendu à l'ensemble des services de communications électroniques et permette par exemple à un utilisateur de bloquer l'envoi de tout moyen d'identification de son équipement; ainsi par exemple l'envoi de données créées par des *cookies* ou par les systèmes d'identification d'un élément de son terminal (par ex. via un Global Unique Identifier).

(90) Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission : *www.privacy.fgov.be*.

(91) Cf. à ce propos la recommandation de la C.N.I.L. française suivant laquelle tout accès à un site marchand doit être possible sans que l'internaute n'ait à s'identifier préalablement. Sur cette recommandation, lire M. Georges, « Relevons les défis de la protection des données personnelles : l'Internet et la C.N.I.L. - Commerce électronique, marketing et libertés », *op. cit.*, pp. 71 et 72. A cet égard également, Th. Léonard, art. cit., n° 18.

(92) Ainsi, les prestataires de services de certification devront révéler l'identité des personnes qui se cachent sous un pseudonyme; ainsi, les fournisseurs de cartes mobilophoniques prépayées devront-ils garder une trace de l'identité des personnes souhaitant disposer de tels moyens de communication; ainsi, avant de permettre l'accès à Internet, les fournisseurs d'accès devront prendre certaines précautions pour s'assurer de l'identité des demandeurs d'accès.

(93) Projet de loi relatif à la criminalité informatique, *Doc.*, Ch. représ., 0213/013 adopté par la Chambre des représentants le 26 oct. 2000 et renvoyé au Sénat en seconde lecture (disponible sur le site de la Chambre : *www.lachambre.be*).

(94) La notion d'écoute téléphonique doit être entendue au sens le plus large puisqu'il s'agit de toute interception de messages véhiculés par les réseaux de télécommunications. Le projet de loi susmentionné prévoit, par une modification de l'article 109*ter* E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques, l'obligation pour tous les opérateurs de réseaux et les fournisseurs de services de télécommunications (ainsi, les fournisseurs d'accès, les serveurs d'anonymat, les agents de recherche, etc.) de conserver pendant une durée qui ne peut être inférieure à douze mois les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs du service.

(95) Le projet de convention sur la cybercriminalité élaboré par le comité d'experts a été transmis le 16 octobre par le comité des ministres à l'Assemblée parlementaire du Conseil de l'Europe (Doc. 8875). Le texte est disponible sur le site du Conseil : *http://stars.coe.fr/doc00/edoc8875.htm*.

(96) Entendue au sens strict.

(97) Arrêt *Kruslin*, 24 avril 1990, série A, n° 166-A et n° 76.

(98) Sur ces principes, lire notre article, « A propos du projet de loi dit n° 214 - La lutte contre la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves », *in Hommage à J. du Jardin*, Kluwer, Bruxelles, 2001, à paraître, et les nombreuses références y reprises en particulier les références aux avis de la Commission belge de protection de la vie privée, en particulier au n° 33/99 du 13 décembre 1999 concernant des projets de loi relatifs à la criminalité informatique.

(99) Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception de télécommunications, 3 mai 1999, WP. 18; Recommandation 3/99 relative à la protection des données de trafic par les fournisseurs de services internet pour le respect du droit, 7 septembre 1999, WP. 25. Les deux recommandations sont disponibles sur le site : *http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs.htm*. Sur les limites qu'impose le droit constitutionnel nord-américain au « devoir » des opérateurs de service de télécommunications de collaborer avec les autorités policières, lire R. Pepin, « Le statut juridique du courriel au Canada et aux Etats-Unis », *Lex Electronica*, vol. 6, n° 2, 2001 (disponible sur le site : *www.lex-electronica.org/articles/v6-2/pepin.htm.*).

plus aisé de leurs droits. Ce principe peut recevoir de multiples applications : ainsi le droit de la personne concernée peut s'exercer plus aisément par un simple clic sur un sigle permettant l'accès direct à un « privacy statement » (100) reprenant de manière détaillée les informations relatives à l'identité de la personne responsable, aux finalités poursuivies par le traitement, etc. (101). La personne concernée peut être amenée à exercer son droit au consentement ou son droit d'opposition directement en ligne. En ce qui concerne le droit d'accès proprement dit, c'est-à-dire le droit de connaître les données enregistrées, leur origine, la logique du traitement, etc. droit consacré par l'article 10 de notre loi, on peut de même imaginer qu'il s'exerce en ligne par une demande signée électroniquement. Enfin, le droit de recourir en cas de contestation relative à la pertinence ou la qualité d'une donnée, droit consacré par l'article 12, pourquoi ne pas permettre son exercice, voire sa résolution, par des mécanismes électroniques de saisine et de règlement des conflits. De tels mécanismes dits de cybermagistrature (102) prônés par la directive sur certains aspects du commerce électronique (103) et déjà acceptés par la Commission dans le cadre des accords conclus avec les Etats-Unis relatifs aux « Safe Harbor Principles » (104) peuvent parfaitement s'appliquer en la matière. Le principe en effet est le même : dans la mesure où le problème est créé par l'utilisation d'Internet, il doit être résolu en prenant en considération la même technologie dans la mesure où celle-ci peut offrir une solution plus rapide, garantie par un tribunal indépendant et à la suite d'une procédure contradictoire. Il va de soi que cette possibilité n'exclut pas le droit de chacun de saisir une juridiction officielle

C. — **Le droit à une technologie *privacy compliant***

27. — La recommandation 1/99 du 23 février 1999 (105), émise par le groupe dit de l'article 29, sur la base d'une analyse des risques créés pour la vie privée par les logiciels et matériels utilisés pour la communication sur Internet, a émis le principe suivant lequel l'industrie du logiciel et du matériel se devait de développer des produits en conformité avec les dispositions des directives de protection des données personnelles. Cette recommandation trouve un écho remarquable dans la récente proposition de directive qui prévoit en son article 14.3 que « en tant que de besoin, la Commission adopte des mesures afin de garantir que les équipements terminaux comportent les sauvegardes nécessaires pour assurer la protection des données à caractère personnel et le respect de la vie privée des utilisateurs et des abonnés,... » (106). Cette interdiction des technologies *privacy killing,* selon l'expression de J.-M. Dinant, peut se déduire aussi de l'obligation légale imposée à tous les responsables de traitement de prévoir des mesures de sécurité organisationnelles et techniques appropriées aux risques engendrés pour la protection des données. Ainsi, le responsable d'un site se doit de veiller à la confidentialité des messages échangés avec le site, à signaler clairement à l'internaute les transmissions de données, fussent-elles automatiques comme c'est le cas par les hyperliens avec des sociétés de *cybermarketing*, et à lui donner les moyens techniques de bloquer de telles transmissions.

28. — Peut-on aller plus loin et recommander le développement de « privacy enhancing technologies » (107), pour reprendre la même terminologie, c'est-à-dire d'outils ou de systèmes qui permettent de mieux assurer le respect du droit des personnes concernées? La question est ouverte. Il est certain que c'est sans doute le marché qui, librement, développera ces technologies et que le rôle de l'Etat, subsidiaire en la matière, sera de promouvoir de telles technologies en informant le public de leur existence, voire en s'assurant de leur accessibilité à un prix abordable. Le cas du système P3P (Privacy Preferences Platform), développé par l'industrie américaine et repris par le World Wide Web Consortium, est intéressant à cet égard. Ce système permet à chaque internaute de définir ses propres préférences, et à partir de là, soit de restreindre son accès aux seuls sites respectant ces préférences, soit de négocier librement avec les autres sites (108). Ce système a fait l'objet d'une analyse par le groupe dit de l'article 29 et son utilisation pourrait être généralisée soit par l'incorporation du système dans les systèmes de navigation, soit comme service à valeur ajoutée offert entre autres à leurs clients par les fournisseurs d'accès. En conclusion, note à juste titre la Commission belge de protection de la vie privée (109), si chaque acteur doit intégrer, au stade du traitement auquel il participe, les principes de protection des données à caractère personnel, la Commission constate que les industries du *software*, du *hardware*, ainsi que les responsables de l'élaboration des protocoles et des standards techniques utilisés pour transmettre des informations en réseau, ont un rôle primordial à jouer dans la configuration des produits et services mis sur le marché. Eu égard aux possibilités qu'offrent les nouvelles technologies, celles-ci devraient non seulement permettre l'élaboration de produits :

— conformes au cadre légal, par exemple par la transmission par les navigateurs Internet du minimum d'informations nécessaires à une connexion, ou par l'adoption de mesures de sécurité adéquates; mais également;

(100) A propos de ces *privacy statements* ou *policies*, lire S. Louveaux, « Le commerce électronique et la vie privée », colloque A.B.J.E., pp. 183 et s. Cf. également leur étude détaillée par le groupe d'experts sur la sécurité de l'information et la vie privée, *in* « Projet d'étude sur les instruments et mécanismes relatifs à la mise en œuvre sur les réseaux globaux des lignes directrices de l'O.C.D.E. en matière de vie privé », O.C.D.E., Paris, 18 et 19 mai 1998, DSTI/ICCP/REG(98)6.

(101) On peut songer à un accès direct au site de l'organe ayant procédé à l'audit du site dans le cadre de la labellisation de celui-ci ou au site de l'autorité de contrôle auprès duquel le responsable des traitements effectués par le site a dû nécessairement opérer la déclaration prévue par l'article 17 de la loi de 1992 (cette dernière idée a été proposée par la Commission belge de protection de la vie privée lors de son avis à propos de l'arrêté royal n° 18 relatif aux déclarations). Sur l'utilisation des labels *privacy* comme moyen de garantie effective de la protection des données, lire J. Reidenberg, « Adapting Labels and Filters for Data Protection », *Cybernews*, 1997, III, 6 disponible au site de *Lex electronica* : *www.droit.montreal.ca/pub/cybernews/.*

(102) Sur ces mécanismes de cybermagistrature, lire notamment, M. Antoine, D. Gobert, A. Salaun, « Les nouveaux métiers de la confiance », *in* « Droit des technologies de l'information - Regards prospectifs », E. Montero (ed.), *Cahiers du C.R.I.D.*, n° 16, 1999, pp. 24 et s., n^os 40 et s.

(103) L'article 17 dispose que les Etats membres veillent à ce que : « leur législation permette en cas de conflits entre un prestataire et un destinataire d'un service de la société de l'information, l'utilisation effective de mécanismes de résolution extrajudiciaire, y compris par les voies électroniques appropriées ».

(104) Cf. *supra*, n° 19.

(105) l s'agit de la recommandation 1/99 du 23 février 1999 sur les traitements invisibles et automatiques de données personnelles sur Internet réalisés par des logiciels et matériels (disponible au site déjà cité). Le groupe de l'article 29 y avait décrit très précisément les caractéristiques du fonctionnement des logiciels de navigation et matériels utilisés pour la communication sur Internet qui représentaient des risques pour la vie privée.

(106) Il s'agit ici d'une application des mesures par ailleurs prévues par l'article 3.3, point *c*, de la directive 1999/5/C.E. sur les équipements terminaux qui prévoit explicitement la possibilité d'exiger des fabricants de terminaux le respect des exigences essentielles au rang desquelles figure la protection de la vie privée. Cette idée d'utiliser la directive dite Terminaux aux fins de promouvoir des systèmes « privacy compliant » avait été émise dans le cadre des travaux d'Eclip (cf. en particulier mes conclusions : « Internet and Privacy : any conclusions », prononcées lors du premier séminaire Eclip, mai 1999, disponible sur le site : *www.droit.fundp.ac.be/crid.*, et surtout J. M. Dinant, « Law and Technology Convergence in the Data Protection Field? », rapport déjà cité, pp. 22 et s.).

(107) L'expression a été utilisée pour la première fois en août 95 par le rapport commun de l'Information and Privacy Commission de l'Ontario et de la Registratiekamer des Pays-Bas, Privacy Enhancing technology : The path to Anonimyty, Achtergrondstudies en Verkenningen 11, Den Haag, 2 vol., Nov. 98 (2e édition) disponible sur le site : *www.registratiekamer.nl.* Sur ces P.E.Ts, lire également, les réflexions d'H. Burkert, « Privacy Enhancing Technologies, in Privacy : quels risques », *Cahier du C.R.I.D.*, n° 13, Story-Scientia, 1997, pp. 91 et s. et les réflexions du groupe d'experts de l'O.C.D.E. déjà citées, n^os 49 et s.

(108) La description du système P3P peut être trouvée sur le site : *www.w3.org*.

(109) Avis d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique, avis n° 34/2000, disponible sur le site de la Commission : *www.privacy.fgov.be*. Cf. sur tous ces points les travaux de J.-M. Dinant déjà cités et le rapport à paraître du groupe d'experts en matière technique créé au sein du groupe de l'article 29, cité note 16.

— qui facilitent l'application des principes et qui permettent par exemple un accès direct par le particulier à ses données ou un droit d'opposition automatique;

— et qui améliorent le niveau de protection des données à caractère personnel; de nouveaux outils, plus connus sous le nom de *privacy enhancing technologies* ont pour vocation de limiter ou d'empêcher la collecte de certaines données par des moyens techniques : c'est en particulier la vocation des serveurs *proxy*, des logiciels de destruction des *cookies*, des logiciels permettant l'anonymat ou des filtres *e-mail*.

D. — **La vie privée sur Internet, droit du consommateur**

29. — La banalisation de l'utilisation d'un outil autrefois réservé aux seules entreprises, la généralisation de son usage dans le domaine du commerce électronique induisent une approche plus consumériste de la protection de la vie privée. C'est en effet en sa qualité de consommateur que l'internaute ressentira les atteintes à la protection de sa vie privée. Ainsi se verra-t-il noyé de courriers non sollicités, une publicité parfaitement ciblée sur ses habitudes de consommation lui sera adressée. L'accès à certains sites et les prix qui lui seront proposés (110) risquent également d'être conditionnés par ce profil. Cette constatation explique que les premières tentatives américaines de réglementation législative (111) aient concerné la protection de la vie privée des consommateurs en ligne. C'est au nom de la défense des consommateurs que la Federal Trade Commission américaine (112) a fondé une jurisprudence intéressante en matière de protection des données et, plus récemment, en a proposé la réglementation législative (113). En Europe, la lutte contre le *spamming*, déjà évoquée (114), a été ouverte dans le cadre d'une directive relative aux contrats à distance relevant du champ de la protection des consommateurs et, à l'inverse, la disposition de l'article 14 de la directive consacrée par notre article 12 de la loi sur la vie privée (115), en édictant le droit d'opposition à toute utilisation des données personnelles à des fins de prospection commerciale (116), protège le droit des personnes concernées autant sur le plan de ses intérêts économiques de consommateur que de ses libertés.

30. — Cette convergence des intérêts de protection économique des consommateurs et des libertés des citoyens ouvre des perspectives intéressantes. Les associations de protection des consommateurs étendent de plus en plus leur préoccupation au domaine du respect de la vie privée et demain constitueront sans doute des groupes de pression puissants, militant pour un tel respect. Surtout, cette convergence augure de la possibilité d'utiliser les « armes » bien connues en matière de protection des consommateurs sur le terrain de la défense de la vie privée. On songe en particulier à l'utilisation des moyens de recours collectifs contre des entreprises offrant des services sur le Net et ne respectant pas les droits des personnes concernées-consommateurs ou utilisant des méthodes de publicité déloyale telles certaines pratiques de *cybermarketing*.

(110) Sur ces dérives permises notamment par les traitements invisibles, *supra* n° 5. A noter la vision prophétique de G. Marx dès 1991 (« Privacy and Technology », *Whole Earth Rev.*, 1991, pp. 90 et s.) : « Purchasers of pregnancy testing kits may receive sollicitations from pro- or anti-abortion groups... Purchasers of weight-loss products or participants in diet programs may be target for promotional offers from sellers of candy, cookies and ice cream, or conversely... Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organizations, or face employment denial, harassment and even blackmail... ».

(111) Comme en témoigne la multiplication depuis 1995, des projets (Bills) de législations intitulées « Consumer Online Privacy Act ».

(112) La compétence de la F.T.C. en matière de protection des consommateurs est non une compétence directe mais une compétence indirecte de comportement loyal et non trompeur d'organisations vis-à-vis de consommateurs lorsque ces organisations émettent un « descriptive or false » statement.

(113) Cf. le rapport au Congrès, « Privacy Online Fair Information Practices in the Electronic Market place », May 2000, disponible au site de la F.T.C. : *www.ftc.gov/os/2000/05/index.htm*.

(114) *Supra*, n° 16.

(115) Cf. la directive 97/7 du 20 mai 1997 dite « Vente à distance » qui, en son article 10, stipule que l'utilisation d'automates d'appel et de téléfax pour l'envoi de publicités est soumise au consentement préalable du consommateur.

(116) Il s'agit ici d'une formule d'*opt-out.* On notera que la proposition de directive préalablement étudiée (*supra*, n° 13) substitue à ce système celui de l'*opt-in*.

Bref, le droit à la protection des données a tout à gagner de l'utilisation du levier que lui offre le droit de la consommation.

C. CONCLUSIONS

31. — Le débat « Internet et vie privée » est crucial au regard des risques nouveaux créés par l'étendue et les caractéristiques d'Internet. Sa solution oblige à réévaluer les principes de base de nos législations à l'aune de ces risques, voire à oser des législations nouvelles tenant compte des progrès et de la convergence des technologies. Elle oblige surtout à ouvrir de nouveaux champs d'investigation : il est clair que la loi ne peut plus être la solution unique mais doit renvoyer à d'autres solutions. D'une part, l'autorégulation (117) est certes une source complémentaire qui permet aux milieux professionnels multiples (le monde du *cybermarketing*, celui des fournisseurs d'accès, celui des services de recherche ou des opérateurs de réseaux) de développer des solutions plus adaptées apportant une valeur ajoutée aux principes souvent vagues de nos législations. Ces solutions, élaborées au plan national, régional ou international, doivent être établies dans toute la mesure du possible en concertation avec les autres acteurs intéressés : les représentants des consommateurs, les associations de libertés, etc. D'autre part, les normes techniques constitueront demain plus encore qu'aujourd'hui le moyen le plus adéquat de trouver des solutions plus respectueuses de la liberté de choix de chacun et de sa vie privée (118). C'est le devoir des autorités chargées de la protection des données de pénétrer les forums où se discutent les choix d'infrastructure technique des réseaux, les protocoles de communication et les caractéristiques de nos logiciels de navigation.

32. — Ces débats seront sans doute à mener non plus à un niveau national, mais à un niveau global. Internet est global et on s'aperçoit chaque jour un peu plus de la vanité de toute action législative ou autre menée à un plan purement national. La recherche de consensus au sein d'organes internationaux (119) est une absolue nécessité. Pour y parvenir, les *privacy advocates* peuvent bénéficier du soutien de nouveaux groupes de pression comme ceux des associations de libertés et surtout des consommateurs. Bref, le débat « Internet et vie privée » ne fait que commencer et son ampleur est à la dimension même d'Internet : global et essentiel pour que survivent nos libertés dans la vie de tous les jours.

Yves POULLET
Doyen de la Faculté de droit de Namur
Directeur du C.R.I.D.-F.U.N.D.P.
Professeur à la Faculté de droit de Liège

(117) Sur l'autorégulation d'Internet, sa valeur et ses limites, le lecteur voudra bien se référer à l'article publié par l'auteur : « How to regulate Internet? Self-regulation, Value and Limits », document Eclip, à paraître dans l'ouvrage collectif : *Legal Aspects of E-commerce*, Looselcaf Publishing, London, 2001; Cf. également le rapport de la Federal Trade Commission, « Self Regulation and Privacy Online - A Report to Congress, July 1999 », disponible à l'adresse : *http://ftc.gov/os/1999/9907/privacy.99pdf* et les remarquables écrits de C.-J. Bennett en particulier : le rapport présenté à la conférence de Venise : « Privacy self-regulation in a global economy : A race to the top, the bottom or somewhere else? », publiée dans les *Actes de la Conférence internationale des commissaires à la protection des données,* Venise les 28, 29 et 30 sept. 2000.

(118) Sur ce point les réflexions de J. Dumortier et C. Goemans à propos du rôle des normes tels les standards I.S.O. dans la protection des données, *in* « Data Privacy and Standardization », Discussion Paper prepared for C.E.N./I.S.S.S. Open Seminar on Data Protection, Brussels, 23/24 mars 2000 (disponible au site de l'I.C.R.I. : *www;law.kuleuven.ac.be/icri*).

(119) Nous reprenons ici les conclusions que S. Rodota, le « garante » italien à la protection des données, organisateur de la Conférence internationale de Venise, adressait au terme de cette conférence, prêchant pour une Convention conclue sous l'égide de l'O.N.U.